UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,557	07/26/2001	Donald E. Duval	1875.9080002	9224

26111 7590 09/07/2006

STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/916,557	DUVAL, DONALD E.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,9-11 and 13-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,9-11 and 13-29* is/are rejected.

7)☒ Claim(s) *13* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on June 12, 2006.

   Claims 2, 4-8 and 12 are cancelled. Independent claims 1 and 11 are amended. New claims 23-29 are added. Thus claims **1, 3, 9-11 and 13-29** are pending/examined.

2. Applicant has amended independent claims 1 and 11 and overcomes the 35 U.S.C. 112, first paragraph, (new matter) rejection set forth in the previous office action. Thus this particular rejection is withdrawn.

3. Examiner and Applicant, Lori A. Gordon, (registration # 50,633) conducted, Examiner's initiated interview on Thursday August 31st and Friday, September 1st, 2006. The purpose of the initial interview on Thursday August 31st, 2006 was to discuss independent claim 11, on the possibility of allowing claim 11 with the corresponding dependent claims and making Examiner's amendment . Applicant has agreed with Examiner's recommendation and requested to make some modification on the dependent claims. However the Examiner latter on, found that the subject matter/limitation, considered allowable, incorporated by the amendment onto the independent claim 11, was actually a new matter that is not supported by the original disclosure.
   Examiner on Friday, September 1st, 2006 called the applicant and pointed out, the new matter which is incorporated in the amended independent claim 11, and requested the applicant to review the application and get back to the Examiner. However, Applicant did not respond back to the Examiner.

Response to Arguments

4. Applicant's arguments/remarks filed on June 12, 2006 have been fully considered and they are not persuasive.

Applicant argued that the combination of Vano and Schneier (the references on the record) does not teach or suggest the amended limitation enclosed in the independent claims, in particular, the amended independent claim 11, that is now submitted.

Examiner disagrees with this argument.

Examiner would point out that each and every limitations of the independent claim 11 and 1 except the new matter (see the new matter rejection set forth in this office action below) which is added on claim 11, is disclosed by the combination of the references, namely **Vano and Schneier** as shown below.

Referring to the independent claims 11 and 1 Vano discloses

- An encryption accelerator [Figure 1, ref. Num "550"] (An encryption accelerator met to be "Cryptographic co-processor" shown on figure 1, ref. Num "550") comprising:

- A combinational logic block arranged to perform a pre-determined logic operation on selected input values;[Figure 1, ref. Num "576" and column 6, lines 50-55) ("As explained on column 6, lines 50-55 a Permuter shown on figure 1, ref. Num "576" performs cryptographic operations as explained on column 6, lines 50-55)

- A state memory array[Figure 1, ref. Num "554" or "State Register"] arranged to store a plurality of state memory values;[Column 6, lines 19-22;] (state memory values is met "channel program states")

- A state machine coupled to the state memory array configured to perform of encryption algorithm.[Figure 1, ref. Num "558", "control register"; column 6, lines 31-36]

- Performing a shuffling operations using a portion of the key array, wherein the shuffling operation is performed concurrently with the receipt of a portion of the key array,[Column 6, lines 54-59; Column 6, lines 19-21; column 8, lines 20-24](Permuters select bits from state register as explained on column 6, lines 54-59 and the state register contains channel program as explained on column 6, lines 19-21 and the key is also contained in the channel program as explained on column 8, lines 20-24)

- Byte-wise transferring the data to the combinational logic block as a first input value, and transferring a corresponding state memory value to the combinational logic as a second input value; logically operat on the first and the second input values by the combinational logic to form a resulting/an encrypted data byte;[figure 1](As shown on figure 1, it is implicit to transfer data from the data register "564" and the state register "554" to the permuter which is shown on figure 1, ref. Num "576") and

- Outputting the resulting/encrypted data byte.[Figure 1, ref. Num "566", "data out register"]

Vano does not explicitly disclose

- Initializing via hardware of an incrementing pattern in the state memory array without loading the incrementing pattern from an external memory
- Wherein the shuffling operation is the RC4 shuffling operation,
- Byte-wise transferring of data

However, in the same field of endeavor, **Schneier** discloses

- Storing of an incrementing pattern in the state memory array with/without loading the incrementing pattern from an external memory [Page 397, lines 23] (filling the s-box linearly)
- Wherein the RC4 shuffling operation includes moving each of the plurality of state memory values based upon the secret key.[Page 397, lines 23-page 398 line 3]
- Byte-wise transferring of data [Page 397, lines 21-23](S-box-entries are exclusively OR'd byte-wise with plaintext)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of the ARCFOUR or RC4 encryption algorithm per teachings of **Schneier** into the configurable cryptographic processing engine and method as taught by **Vano** in order to provide a faster encryption.(It is known that encryption is fast about 10 times faster than DES, see page 397, line 22)

As to the argument made to the rest of the claims, Examiner would point out that dependent claims stands and falls with the corresponding independent claims.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. **Independent Claims 11 and the new dependent claims 23-24 ; 26-27** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification/original disclosure fails to mention/specify or teach the following limitation, which is added into the independent claims 11. Part of the following limitation is also recited in the new dependent claims 23-24 and 26-27, "**generate a pseudo-random number as a result of a second RC4 shuffling operation**; byte-wise transfer a portion of the data to the combinational logic block **as a first input value**, **transfer the generated pseudo-random number to the combinational logic as a second input value**,". These limitations are considered/found to be a new matter.

For the purpose of examination, the office has fully considered/examined all the limitations in the above claims, except the limitation indicated above as a new matter.

7. **Claims 13-22 and 28-29** depend from the rejected independent claim 11 and 27 respectively, and include all the limitations of the respective claims, thereby

rendering those dependent claims failing to comply with the written description requirement.

For the purpose of examination, the office has fully considered/examined all the limitations in the above claims, except the limitation indicated above as a new matter.

Claim Objections

8. Dependent Claim 13 is objected to because of the following informalities: Claim 13 is dependent on the canceled claim 12. For the purpose of Examination claim 13 is considered to depend on claim 11 instead of claim 12.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

9. **Claims 1, 3, 9-11 and 13-29** are rejected under 35 U.S.C. 103(a) as being unpatentable over by Johns-Vano (hereinafter refereed as "**Vano**) (European Patent Publication No. "EP 0895164")(Publication date Feb 03, 1999) in view of a book by **Bruce Schneier:** Title "Applied Cryptography" " Chapter 17, "Other Stream Ciphers and Real Random-Sequence Generation" (hereinafter refereed as **Schneier**) (Pages 397-398)(both the references are submitted by the applicant and are included in the applicant IDS)

10. **As per claim 11,13-14, 21-29 Vano** discloses

- An encryption accelerator [Figure 1, ref. Num "550"] (An encryption accelerator met to be "Cryptographic co-processor" shown on figure 1, ref. Num "550") comprising:
- A combinational logic block arranged to perform a pre-determined logic operation on selected input values;[Figure 1, ref. Num "576" and

column 6, lines 50-55) ("As explained on column 6, lines 50-55 a Permuter shown on figure 1, ref. Num "576" performs cryptographic operations as explained on column 6, lines 50-55)

- A state memory array[Figure 1, ref. Num "554" or "State Register"] arranged to store a plurality of state memory values;[Column 6, lines 19-22;] (state memory values is met "channel program states")

- A state machine coupled to the state memory array configured to perform of encryption algorithm.[Figure 1, ref. Num "558", "control register"; column 6, lines 31-36]

  - Performing a shuffling operations using a portion of the key array, wherein the shuffling operation is performed concurrently with the receipt of a portion of the key array,[Column 6, lines 54-59; Column 6, lines 19-21; column 8, lines 20-24](Permuters select bits from state register as explained on column 6, lines 54-59 and the state register contains channel program as explained on column 6, lines 19-21 and the key is also contained in the channel program as explained on column 8, lines 20-24)

  - Byte-wise transferring the data to the combinational logic block as a first input value, and transferring a corresponding state memory value to the combinational logic as a second input value; logically operat on the first and the second input values by the combinational logic to form a resulting/an encrypted data byte;[figure 1](As shown on figure 1, it is implicit

to transfer data from the data register "564" and the state register "554" to the permuter which is shown on figure 1, ref. Num "576") and

- Outputting the resulting/encrypted data byte.[Figure 1, ref. Num "566", "data out register"]

Vano does not explicitly disclose

- Initializing via hardware of an incrementing pattern in the state memory array without loading the incrementing pattern from an external memory
- Wherein the shuffling operation is the RC4 shuffling operation,
- Byte-wise transferring of data

However, in the same field of endeavor, **Schneier** discloses

- Storing of an incrementing pattern in the state memory array with/without loading the incrementing pattern from an external memory [Page 397, lines 23] (filling the s-box linearly)
- Wherein the RC4 shuffling operation includes moving each of the plurality of state memory values based upon the secret key.[Page 397, lines 23-page 398 line 3]
- Byte-wise transferring of data [Page 397, lines 21-23](S-box-entries are exclusively OR'd byte-wise with plaintext)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of the ARCFOUR

or RC4 encryption algorithm per teachings of **Schneier** into the configurable cryptographic processing engine and method as taught by **Vano** in order to provide a faster encryption.(It is known that encryption is fast about 10 times faster than DES, see page 397, line 22)

11. **As per independent claim 1, Independent claim 1** recites the same limitation as that of the independent claim 11 and is rejected by the same analogy/rational as that of the above independent claim 11.

12. **As per claim 3 the combination of Vano and Schneier** discloses a system for encrypting and decrypting data as applied to claim 1 above. Furthemore **Vano** discloses the system further comprising: a storage unit arranged to store at least a portion of the data to be encrypted [Figure 1, reference "564", date in register "564"; column 6, lines 44-47]

13. **As per claim 9-10 the combination of Vano and Schneier** discloses a system for encrypting and decrypting data as applied to claim 1 above. Furthemore **Vano** discloses the system further comprising an external memory [figure 1, reference "12"] coupled to the state memory arranged to store selected state memory values. [As explained in claim 1, about "channel program" see column 4, lines 29-33]

14. **As per claim 15-19,** the combination of **Vano** and **Schneier** discloses the system as applied to claim 1 above. Furthermore **Vano** discloses an input latch and output latchs of the encryption acceleration.[figure 1; Column 6, lines 44-46](data in register shown on figure 1, ref. Num "564"and the data out register shown on figure 1, reference "566" are met to be as the input and output latches of the encryption accelerator. The microsequencer 302 of the CPU) loads data into and from the registers as shown on Column 6, lines 44-46)

15. **As per claim 20,** the combination of **Vano** and **Schneier** discloses the system as applied to claim 1 above. Furthermore **Schneier** discloses the system wherein the accelerator further includes a first index counter and a second index counter . [Page 397, lines 14-page 398 line 10]

Conclusion

16. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-2723806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
08/28/2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100